December 2019

Former CIA Officer Sentenced to 19 Years in Prison for Conspiracy to Commit Espionage

Former Central Intelligence Agency case officer Jerry Chun Shing Lee was sentenced on November 22 to 19 years in prison for his role in a conspiracy to communicate, deliver, and transmit national defense information to the Chinese government. In a case demonstrating the threat posed by Chinese intelligence services targeting former U.S. security clearance holders for recruitment, Lee admitted in his May plea agreement Chinese intelligence officers approached him three years after he left the CIA, tasked him to provide sensitive information about his former employer, paid him hundreds of thousands of dollars, and offered to take care of him "for life" in exchange for his cooperation. In response to the Chinese intelligence officers' requests, Lee admitted he created a document containing national defense information related to the CIA, including the location of a sensitive operation. In addition, notes Lee possessed detailed intelligence provided by CIA assets, true names of assets, operational meeting locations and phone numbers, and information about covert facilities. He also admitted he deliberately concealed and failed to disclose information during a series of interviews with the FBI and CIA. Read about the sentencing.

Former Monsanto Employee Indicted on Economic Espionage and Theft of Trade Secrets Charges

A federal grand jury in the Eastern District of Missouri returned an eight-count indictment on November 21 charging Chinese national Haitao Xiang with economic espionage, theft of trade secrets, and other violations for his alleged role in a conspiracy to steal valuable intellectual property from his former employers, Monsanto and its subsidiary, The Climate Corporation. According to the indictment, Xiang was reportedly a member of a talent plan—a Chinese government program offering researchers incentives to work in China to advance the country's science and technology capabilities. Within one year of his recruitment into the talent plan, Xiang allegedly resigned from his position with Monsanto and attempted to travel to China with valuable intellectual property regarding the company's Nutrient Optimizer, a proprietary algorithm used to improve farmers' agricultural productivity. Xiang was intercepted at the airport before he could board a one-way flight with the trade secrets allegedly in his possession. If convicted, he faces up to 15 years in prison and a $5 million fine for each economic espionage charge and up to 10 years in prison and a $250,000 fine for each theft of trade secrets charge. Read about the charges.

U.S. Citizen Arrested for Assisting North Korea in Evading Sanctions

U.S. citizen and Singapore resident Virgil Griffith was arrested on November 28 and charged via a criminal complaint for his alleged role in a conspiracy to help North Korea evade sanctions, in violation of the International Emergency Economic Powers Act. According to court documents, although the U.S. Department of State denied him permission to travel to North Korea, Griffith delivered a presentation and provided technical expertise at a conference in Pyongyang regarding the use of cryptocurrency and blockchain technology to launder money and evade sanctions. He then allegedly devised plans to illicitly exchange cryptocurrency between North and South Korea, encouraged other American citizens to travel to North Korea to attend the conference, and announced plans to renounce his U.S. citizenship. If convicted, Griffith faces up to 20 years in prison. Read about the charges.

Five Individuals and Three Companies Charged in Conspiracy to Evade International Trade Sanctions

A superseding indictment unsealed on December 1 in U.S. District Court for the Southern District of Georgia charged one U.S. citizen, two Russian nationals, two Italian nationals, and three companies for their alleged roles in a scheme to obtain sensitive U.S.-origin technology on behalf of a business controlled by the Russian government, in violation of the International Emergency Economic Powers Act. According to the indictment, Oleg Vladislavovich Nikitin, Anton Cheremukhin, Gabriele Villone, Bruno Caparini, and Dali Bagrou allegedly conspired to purchase a $17 million power turbine from a U.S. manufacturer for use on a Russian Arctic deepwater drilling platform. To evade export laws prohibiting the turbine's sale to Russia for national security reasons, the defendants allegedly falsified documentation and employed an Italian company to conceal the purchase. If convicted, the individuals face up to 20 years in prison for each count and financial penalties ranging from $250,000 to $1 million per charge. Read about the charges.

Former U.S. Navy Contractor and Its President Sentenced for Scheme Related to Transfer of U.S. Navy Submarine Rescue Technology

Former defense contractor OceanWorks International Corp. and its president, Glen Omer Viau, were sentenced on December 2 in U.S. District Court for the District of Columbia for their roles in a scheme to transfer export-controlled technical data to China. A Houston-based subsea technology company that served as a prime contractor for the U.S. Navy, OceanWorks was acquired in 2016 by a Chinese company affiliated with the People's Liberation Army Navy—an acquisition concealed by the use of a series of front companies. As he admitted in his plea agreement, Viau then joined OceanWorks as its president and participated in a conspiracy to transfer data regarding a U.S. Navy submarine rescue system to the Chinese parent company for use in a proposal to build a similar system for the PLA Navy. He subsequently concealed information about OceanWorks' export violations and affiliation with the PLA Navy from the U.S. Department of Commerce and the U.S. Navy. As the result of investigative collaboration between the United States and Canada, the company was banned from contracting with the U.S. government and the Canadian government ordered the divestiture of the OceanWorks acquisition by the Chinese front companies. In U.S. District Court, the company was fined $84,000, and Viau was ordered to pay a $25,000 fine and sentenced to time served. Read about the sentencing.

FBI Official Discusses Strategic Threat Posed by China During Senate Hearing

Assistant Director John A. Brown, head of the FBI's Counterintelligence Division, joined other U.S. government leaders on November 19 before the U.S. Senate's Permanent Subcommittee on Investigations for an open hearing titled "Securing the U.S. Research Enterprise from China's Talent Recruitment Plans." During the hearing, Mr. Brown discussed the Chinese government's efforts to acquire American technology and expertise to erode the United States' competitive advantage and supplant it as a global superpower. Watch a video of the hearing or read Mr. Brown's statement for the record.

MEDIA HIGHLIGHT

The following information has been prepared by outlets outside the U.S. government and has not been corroborated by the FBI or its partners. It is presented here for your situational awareness.

Detroit News Highlights Arrest of Visiting Scholar Accused of Stealing Trade Secrets for Iran

An article published on November 6 by the *Detroit News* detailed the arrest of hardware engineer Amin Hasanzadeh, an Iranian military veteran and visiting scholar at the University of Michigan, for allegedly stealing sensitive, confidential data about an aerospace industry supercomputer from a U.S. company. According to the article, a recently unsealed criminal complaint charged Hasanzadeh with stealing the trade secrets and emailing them to his brother, an electrical engineer in Iran, in violation of a nondisclosure agreement developed by the company and a partner firm. Read the *Detroit News* article.